EFFICIENT TECHNIQUES FOR SHARING A SECRET

ABSTRACT OF THE DISCLOSURE

An *n* person secret sharing solution computes *n* unique keys to be distributed to the secret owners along with an exponentiated version of the secret. The custodian performs an exponent / modulo operation each time one of the keys is received from one of the secret owners. Alternatively, *n*+1 keys are created by the custodian, and the custodian retains one key after distributing the remaining *n* keys to the secret owners. After the custodian has received and processed the *n* keys from the secret owners, he performs an exponent / modulo operation using his own retained key. According to another aspect, a *k* out of *n* secret sharing solution involves computing and storing a database having an entry for each unique combination of *k* keys that could be returned from among the *n* keys. After *k* keys have been received, the custodian looks up in the database the entry corresponding to the particular unique combination of secret owners who returned keys. The custodian performs another exponent / modulo operation using the entry retrieved from the database in order to reconstruct the original secret. According to an embodiment, the custodian computes *n*+1 keys, distributes *n* of the keys to the secret owners, and keeps one of the keys for himself. The custodian retrieves his own key and performs a final exponent / modulo operation in order to reconstruct the original secret. According to another aspect, a *k* out of *n* secret sharing solution involves encrypting the original secret before applying any conventional *k* out of *n* secret sharing solution.